National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Metadata Management Capability

Version 1.1.1

IA Metadata Management is the maintenance of IA metadata schemas and the generation, validation, association, and maintenance of IA metadata. The management of IA metadata specifically is the focus of this Capability.

07/30/2012

CGS Metadata Management Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Metadata is data about data. It is used to describe characteristics of data assets to enhance their value and usability. There are many different types of metadata. Some of these types include the following:

1. Discovery metadata–Helps entities find data assets
2. Mission metadata–Describes data assets in their mission context
3. Information assurance (IA) metadata–Encompasses any metadata associated with the protection of a data asset. This can include metadata describing a data asset's security properties, protection requirements, applied protections, and provenance (source of an entity). IA metadata enables data consumers to assess the trustworthiness of the data, while allowing providers to specify controls for their data.

IA Metadata Management is the maintenance of IA metadata schemas and the generation, validation, association, and maintenance of IA metadata. The management of IA metadata specifically is the focus of this Capability.

IA metadata is needed to realize information sharing objectives. Assured information discovery and retrieval hinges on resource attributes that can be conveyed in IA metadata and are sharable across domains. IA metadata supports interoperability for human understanding of data assets and for processing by automated systems, such as discovery services and access control functions. To fully realize interoperable secure information exchange, Enterprises must adhere to the following: a common and consistent Community-approved controlled IA vocabulary (i.e., standard meaning and vocabulary for security or sensitivity markings, specification of format for IA metadata, specification of subject roles and attributes), a robust information sharing infrastructure to protect both data assets and IA metadata, and a set of tools and protocols that facilitates the adoption of IA metadata standards (e.g., cryptographic binding, IA metadata validation) within and across Enterprise boundaries.

IA metadata supports the assessment of the authoritativeness and trustworthiness of data assets that are used by mission supporting entities. This provides the information needed for continuing protection of those data assets. Trustworthiness assessment includes

identifying the extent to which the data asset should be protected from unauthorized disclosure and from unauthorized or unintentional modification while being processed, stored, or exchanged. The IA metadata and the use of IA for metadata and data assets can be afforded the same authoritativeness and trustworthiness as the data asset, and thereby be relied on to formulate decisions.

Like all data, IA metadata needs to be protected using appropriate data protection techniques. IA metadata can be embedded within a data asset, stored alongside a data asset, or stored separately from its associated data asset (e.g., in a repository). Regardless of where IA metadata is stored, all security protections must still apply, such as those provided under the System Protection, Data Protection, and Communication Protection Capabilities, among others.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

IA Metadata Management is carried out by the establishment and subsequent enforcement of policies and procedures for controlling the entities where IA metadata is stored and processed. These policies and procedures oversee the generation and tagging, validation, association, and maintenance of IA metadata.

Generation–Establishes the initial metadata for new and legacy data assets based on policy and schemas established by the Enterprise. These policies and schemas shall comply with established Community standards, where possible. As existing data assets change and move, additional pieces of IA metadata are generated, where applicable.

Tagging–Is a type of generation. The IA metadata tagging function shall create IA metadata that describes the subject data, as defined by the Enterprise retaining the data asset. For example, IA metadata tags may contain the security attributes or provenance of a data asset.

Validation–Establishes the correctness of each instance of IA metadata based on any applicable schemas or business rules. To use IA metadata to make decisions, it shall be

well formed and follow policy. The validation system provided by the Enterprise shall examine all IA metadata to ensure that it follows the correct syntax and complies with the appropriate policies.

Association–Establishes a verifiable relationship between one or more data assets and the IA metadata that describes them. This relationship could be simple or complex, depending on how many data assets and how much IA metadata is involved. The ability to capture and establish the strength of associations between data is crucial in validating and trusting the authoritativeness of the association. The Enterprise shall have a system to perform this function with the ability to automatically monitor and update associations as needed.

Maintenance–Handles the deletion, downgrade, modification, and archiving of IA metadata. Every Enterprise shall have a system to perform IA metadata maintenance. Interoperability promotion shall be one of the ultimate goals of IA Metadata Management. The Enterprise shall use Community-established interchange standards so systems can transfer information between them while maintaining proper protection for all data assets and IA metadata.

All IA metadata functions shall be designed to require a minimum of human interaction. Where possible, IA metadata processes shall be completely invisible to the end user.

Each Enterprise shall establish a set of policies for storing IA metadata used for provenance. These policies will determine whether provenance is stored and, if it is, specifically what, how, and where it is stored.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. All data controlled or shared by the Enterprise is created or tagged with IA metadata.
2. IA metadata can be used by access management systems to make access control decisions.
3. The data asset and IA metadata integrity and authenticity are checked prior to being accessed (e.g., cryptographic binding).

4. Policy that either conveys or describes how to calculate protection requirements for the data asset and associated metadata are part of the authorization and access control decision.
5. When possible, the Enterprise will use standardized data-encoding specifications.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability specifies the protections, while other Community Gold Standard Capabilities enforce them.
2. The Capability enables assured information sharing.
3. The Capability enables finer grained access control to the data asset level (e.g., object, file, row in a database).
4. IA metadata/data associations will be created so tampering can be identified and trust in and integrity of data assets and IA metadata can be ensured.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

In an IA Metadata Management implementation, each Enterprise will have a system in place for generating, validating, and maintaining all IA metadata used by the Enterprise. All applicable data asset protection measures also will apply to IA metadata. Different Enterprises may store IA metadata differently (e.g., embedding within data assets, stored alongside data assets, stored separately in a repository). This is acceptable provided there are policies in place to maintain Community-wide IA metadata interoperability requirements and consistency in IA metadata and data asset protection.

Organizations will use IA metadata for access control and discovery services to achieve information sharing among the Community members. The use of IA metadata supports IA functions that protect the confidentiality, integrity, and availability of data assets and their associated IA metadata. The systems and components that create, use, and manage IA

metadata make up the IA Metadata Management infrastructures that support mission systems.

One of the ways access control decisions are made by a system is based on information found in the IA metadata for a data asset. Each Enterprise will establish a process that is followed if IA metadata is to be used for this purpose. The IA metadata is standardized to Community-wide IA metadata specifications for appropriately applying tags and other IA metadata functions so that the system can readily use the IA metadata to make access control decisions quickly and without error.

Each Organization will establish a framework to oversee the storing of provenance for data assets. The concept of provenance deals with keeping track of a data asset's history, its edits, where it has been, who has had contact with it, and where else it has been used or cited. All of this provenance data is stored as IA metadata. Provenance covers a broad range of information and each individual Enterprise will have to determine how much provenance data to store. Storing provenance data for a wide array of events can take up a large quantity of storage space. Necessary considerations are made to account for this, such as the use of databases and index services. Provenance data can have varying security levels and may be classified differently than its associated data asset and will be handled accordingly. The Community Gold Standard does not dictate what or how much provenance data will be stored, only that each Enterprise will have a policy governing it.

The integrity of the association between data assets and their IA metadata will be assured. This is to prevent the mix up or loss of IA metadata from its correct data assets, which is especially important when IA metadata elements serve as decision criteria. This function creates a level of trust in both the association and the authenticity of the association so that there can be confidence in decisions rendered by Enterprise services, such as access control or attribute-based privilege management systems. One such way the integrity of this association can be maintained is by cryptographically binding data assets to their IA metadata. Cryptographic binding may also be used to verify the integrity and authenticity of all bound assets.

Some data assets have IA metadata embedded within themselves. Each Enterprise will have a system that scans data assets for embedded IA metadata, parses through their contents, and recreates any IA metadata found for storage separate from the data asset, where appropriate. This is an invaluable capability for Enterprises that use centralized IA metadata repositories. There are also legacy data assets that have very little or no

associated IA metadata. This system will also be able to analyze these data assets and create any applicable IA metadata that is missing. For example, the IA subcomponent of the Automated Metadata Population Service (AMPS IA) parses through data assets and populates the security field for a Department of Defense (DoD) Discovery Metadata Specification (DDMS) metadata card, which is an Extensible Markup Language (XML) file. This XML file contains Intelligence Community (IC) Information Security Markings (ISM) based on security classification tokens maintained by the Controlled Access Program Coordination Office (CAPCO). The key here is that this is machine-readable information, stored as IA metadata, about the contents of a data asset. That this is machine readable is important because it means that it can be used by automated systems. There will be a system for creating all types of IA metadata, in human- and machine-readable format, used by systems in the Enterprise.

Every Enterprise will have a system to perform IA metadata-related analysis. Specifically, this system will analyze data assets and will make suggestions on how to classify the asset based on a set of rules. If a suggestion is accepted, the data asset will be tagged using IA metadata in accordance with the classification. The analysis system will also parse through data assets and IA metadata and generate additional metadata for indexing purposes and to simplify future search and discovery.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Portfolio Management–The Metadata Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Metadata Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Metadata Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Metadata Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Metadata Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Metadata Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Metadata Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Metadata Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Metadata Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Metadata Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Communication Protection–The Metadata Management Capability relies on the Communication Protection Capability to protect IA metadata during data transfers.

- Data Protection–The Metadata Management Capability relies on the Data Protection Capability to provide protection mechanisms for IA metadata.
- Risk Mitigation–The Metadata Management Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
AC-4 *INFORMATION FLOW ENFORCEMENT*	Enhancement/s: (1) The information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions. (6) The information system enforces information flow control on metadata. (15) The information system, when transferring information between different security domains, detects unsanctioned information and prohibits the transfer of such information in accordance with security policy. Supplemental Guidance: Actions to support this enhancement include: checking all transferred information for malware, implementing dirty word list searches on transferred information, and applying the same protection measures to metadata (e.g., security attributes) that is applied to the information payload. (17) The information system– a. Uniquely identifies and authenticates source and destination domains for information transfer b. Binds security attributes to information to facilitate information flow policy enforcement c. Tracks problems associated with the security attribute binding and information transfer.
AC-16 *SECURITY ATTRIBUTES*	Control: The information systems supports and maintains the binding of [Assignment: organization-defined security attributes]

	to information in storage, in process, and in transmission. Enhancement/s: (1) The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined. (2) The information system allows authorized entities to change security attributes. (3) The information system maintains the binding of security attributes to information with sufficient assurance that the information–attribute association can be used as the basis for automated policy actions. (4) The information system allows authorized users to associate security attributes with information. (5) The information system displays security attributes in human-readable form on each object output from the system-to-system output devices to identify [Assignment: organization-identified set of special dissemination, handling, or distributions instructions] using [Assignment: organization-identified human readable, standard naming conventions].
AU-10 *NON-REPUDIATION*	Enhancement/s: (1) The information system associates the identity of the information producer with the information. (2) The information system validates the binding of the information producer's identity to the information. (3) The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released. (4) The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.
SC-16 *TRANSMISSION OF SECURITY ATTRIBUTES*	Control: The information system associates security attributes with information exchanged between information systems Enhancement/s: (1) The information system validates the integrity of security attributes exchanged between systems.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Metadata Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD-501, Discovery and Dissemination or Retrieval of Information Within the Intelligence Community, 21 January 2009, Unclassified	Summary: Intelligence Community (IC) elements shall treat information collected and analysis produced as national assets and, as such, shall act as stewards of information who have a predominant "responsibility to provide." ... Stewards shall fulfill their "responsibility to provide" by making all information collected and analysis produced by an IC element available for discovery by automated means by authorized IC personnel, ... (Metadata are the visible attributes that enable the information to be discoverable.)
ICD 710, Classification and Control Markings System, 11 September 2009, Unclassified	Summary: This directive addresses the establishment of the IC classification and control markings system as a critical element of IC procedures for protecting intelligence and information, and sources and methods while ensuring that the information is available without delay or unnecessary restrictions. The classification and control marking system enables information sharing and includes all markings added to classified and unclassified information to communicate one or more of the following: classification, compartment, dissemination controls, disclosure or release authorizations, and other warnings.
ICPM 2008-500-1, Information Sharing Data Standards for Intelligence, unsigned draft, 14 February 2008, Classified	Summary: This manual addresses the establishment of information sharing data standards ... to provide a simple, common way of describing the content, origin, security classification, and file format of intelligence information, making it easier for consumers to discover, access, understand, and use intelligence that is relevant to their needs. Information sharing data standards will be documented at two levels of detail: IC Standards that define the basic concepts associated with the data exchanged in support of specific intelligence missions and functions; and

	Implementation Profiles that provide specific file format details associated with content, metadata, data formats, and controlled vocabularies.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 5015.2, DoD Records Management Program, 21 November 2003, Unclassified	Summary: This directive provides implementing and procedural guidance on the management of records in the Department of Defense (DoD). It sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by the DoD components in implementing their records management programs; defines required system interfaces and search criteria that RMAs shall support; and describes the minimum records management requirements that must be met based on current National Archives and Records Administration (NARA) regulations. Implements DoD 5010.2-STD, which addresses making DoD records visible by developing and registering standardized metadata.
DoDD 8320.02, Data Sharing in a Net-Centric Department of Defense, 23 April 2007, Unclassified	Summary: This directive directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), ... It is DoD policy that data is an essential enabler of network-centric warfare (NCW) and shall be made visible, accessible, and understandable to any potential user in the DoD as early as possible in the lifecycle to support mission objectives. Data assets shall be made visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset. ... Data assets shall be made understandable by publishing associated semantic and structural metadata in a

	federated DoD metadata registry. To enable trust, data assets shall have associated information assurance and security metadata, and an authoritative source for the data shall be identified when appropriate. ...
DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing, 12 April 2006, Unclassified	Summary: This document provides a set of activities that members of communities of interest and associated leadership can use to implement the key policies of DoD Directive (DoDD) 8320.02, Data Sharing in a Net-Centric Department of Defense (DoD). It contains implementation guidance for the Community-based transformation of existing and planned information technology (IT) capabilities across the DoD in support of department-wide net-centric operations. Creating discovery metadata and deploying discovery capabilities that catalog data assets enable users to quickly discover data assets that pertain to specific subjects of immediate interest.
CJCSI 6212.01E, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 15 December 2008, Unclassified	Summary: It is Joint Staff policy to ensure that DoD components develop, acquire, deploy, and maintain IT and National Security Systems (NSS) that (1) meet the essential operational needs of U.S. forces; (2) are interoperable with existing and proposed IT and NSS through standards, defined interfaces, modular design, and reuse of existing IT and NSS solutions; ... A Net-Ready Key Performance Parameter (NR-KPP), consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance (IA), and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. Addresses requirements for making data and services visible by creating and associating ("tagging"), including discovery metadata, for each asset using DoD Discovery Metadata Specification (DDMS) compliant metadata.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, 10 November 2009, Unclassified	Summary: This document outlines a common framework for Identity, Credential, and Access Management (ICAM) within the Federal Government and provides supporting implementation guidance for program managers, leadership, and stakeholders planning to execute a segment architecture for ICAM management programs. It includes courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of ICAM. Federal Identity, Credential, and Access Management (FICAM) mentions Metadata Management as one of five privilege management services.
Executive Branch (EO, PD, NSD, HSPD, …)	
EO 13526, Classified National Security Information, 29 December 2009, Unclassified	Summary: This Executive Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.
Legislative	
Nothing found	

Metadata Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
ICS 500-2 Intelligence Community Standard for Information Resource Metadata, 11 December 2007, Unclassified	Summary: This is a standard for the consistent application, display, and use of information resource metadata that is typically administrative or descriptive and primarily used to support activities such as information creation, storage, management, archiving, downgrading, searching, discovery, cataloging, and categorization. The metadata elements defined are at an abstract or conceptual level from which implementation profiles can be derived.
ICS 500-3 Intelligence Community Standard for Publication Metadata, 11	Summary: This is a standard for the consistent application, display, and use of publication metadata that describes the structural concepts that make up information products, such

December 2007, Unclassified	as the product type, paragraphs, lists, and tables. They are tightly linked to other elements of metadata including information resource metadata and information security marking metadata. The metadata elements defined are at an abstract or conceptual level from which implementation profiles can be derived.
ICS 500-5 Intelligence Community Standard for Source Reference Citation Metadata, 26 June 2008, Unclassified	Summary: This is a standard for the consistent application, display, and use of source reference citation metadata to be applied to intelligence products, information standards, content management and discovery applications, and service transactions where the inclusion of source reference citations benefits the transparency and substantiation of analytical positions. The metadata elements defined are at an abstract or conceptual level from which implementation profiles can be derived.
ICS 500-10 Intelligence Community Standard for Information Security Marking Metadata, 19 August 2008, Unclassified	Summary: This is a standard for the consistent application, display, and use of information security marking metadata to be applied to information products, information standards, content management, service transactions, and discovery applications where information security marking metadata is required. The three primary information security marking metadata elements (Resource Security Mark, Resource Classification Declassification Mark, and Portion Security Mark) defined herein are at an abstract or conceptual level from which implementation profiles can be derived.
ICS 500-21 Tagging of Intelligence and Intelligence-Related Information, currently out for review	Will replace ICS 500-2, ICS 500-3, ICS 500-5, and ICS 500-10.
Implementation Profile for Information Resource Metadata (HTML Encoding), 22 July 2008, Unclassified	Summary: This profile defines detailed specifications for using Hypertext Markup Language (HTML) to encode information resource metadata in compliance with the approved Intelligence Community Standard (ICS) for Information Resource Metadata (ICS 2007-500-3) of 11 December 2007. It further defines the meta name/content attribute pairs captured in an HTML header, mandatory and cardinality requirements, and permissible values for

	representing the information resource metadata concepts in HTML.
Implementation Profile for Information Resource Metadata (XML Encoding), 22 July 2008, Unclassified	Summary: This profile is a statement of the IC's formal adoption of the Extensible Markup Language (XML) encoding from the DDMS, version 2.0, 17 July 2008, to encode information resource metadata in compliance with the approved ICS for Information Resource Metadata (ICS 2007-500-3), 11 December 2007.
Implementation Profile for Information Security Marking Metadata (XML Encoding), 10 August 2008, Unclassified	Summary: This profile defines detailed specifications for using XML to encode information security markings metadata in compliance with the approved ICS for Information Security Marking Metadata. It further defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing the security markings concepts using XML.
Implementation Profile of Intelligence Publications (XML Encoding), 19 August 2008, Unclassified	Summary: This profile defines detailed specifications for using XML to encode publication metadata in compliance with the approved ICS for Publication Metadata. It further defines the XML elements and attributes, associated structures and relationships, mandatory and cardinality requirements, and permissible values for representing the publications concepts using XML. It is the umbrella XML standard for text-based intelligence products for more specific standards such as security markings, source citations, and topical assertions.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Department of Defense Discovery Metadata Specification, version 2.0, 17 July 2008, Unclassified	Summary: This specification defines discovery metadata elements for resources posted to Community and organizational shared spaces. It specifies a set of information fields that is to be used to describe any data or service asset, i.e., resource, that is to be made discoverable to the Enterprise, and it serves as a reference for developers, architects, and engineers by laying a foundation for Discovery Services.

DoD 5015.02-STD, Electronic Records Management Software Applications Design Criteria Standard, 25 April 2007, Unclassified	Summary: This standard sets forth mandatory baseline functional requirements and requirements for classified marking, access control, and other processes, and identifies non-mandatory features deemed desirable for RMA software. Its goal is to make DoD records visible by developing and registering standardized metadata.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
National Information Exchange Model (NIEM) 2.1, 28 September 2009, Unclassified	Summary: National Information Exchange Model (NIEM), a joint venture between the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) with outreach to other government departments and agencies, is an interagency initiative to provide Enterprise-wide information exchange standards and processes that can enable national-level interoperable information sharing and data exchange. Management of metadata is elemental to this initiative.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)

4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Storage requirements–Depending on the implementation decisions, there may need to be additional repositories to store IA metadata (could be the same as where original data assets are stored).
2. Impact/dependency on existing services–This Capability may require other systems to properly generate and update metadata.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Metadata Management Capability.

- The Enterprise shall provide for the management of IA metadata, which provides for the maintenance of IA metadata schemas and the generation, validation, association, and maintenance of IA metadata.
- The Enterprise shall establish the initial metadata for new and legacy data assets based on policy and schemas established by the Enterprise.
- As existing data assets change and move, the Enterprise shall generate additional pieces of IA metadata, where applicable.
- The IA metadata tagging function shall create IA metadata that describes the subject data as defined by the Enterprise retaining the data asset.
- The IA metadata validation function shall ensure that each instance of IA metadata complies with any applicable schemas or business rules, follows the correct syntax, and complies with the appropriate policies.
- The Enterprise shall have the ability to capture and establish the strength of associations between data in validating and trusting the authoritativeness of the association.

- The Enterprise shall have a system by which to automatically monitor and update the associations between data assets and their IA metadata.
- The Enterprise shall have a system to manage the deletion of IA metadata.
- The Enterprise shall have a system to manage the downgrade of IA metadata.
- The Enterprise shall have a system to manage the modification of IA metadata.
- The Enterprise shall have a system to manage the archiving of IA metadata.
- The Enterprise shall use Community-established interchange standards so that systems can transfer information across network boundaries while maintaining proper protection for all data assets and IA metadata.
- IA metadata functions shall be designed to require a minimum of human interaction and be invisible to the end user.
- The Enterprise shall establish policies that govern the storing of IA metadata used for provenance.